WHAT IS CLAIMED IS:

Sub a1

1. A compact personal token, comprising:

a USB-compliant interface releaseably coupleable to a host processing device;

a memory;

a processor, communicatively coupled to the memory and communicatively coupleable to the host processing device via the USB-compliant interface, the processor for providing the host processing device conditional access to data storable in the memory; and

a user input device, communicatively coupled to the processor by a path distinct from the USB-compliant interface, for accepting an input signaling authorization of a processor operation.

2. The apparatus of claim 1, wherein the path is entirely internal to the token.

3. The apparatus of claim 1, wherein the processor operation requires access to private data stored in the memory.

4. The apparatus of claim 3, wherein the private data is designated as requiring authorization before access by an associated identification stored in the memory.

5. The apparatus of claim 1, wherein the input device comprises at least one pressure-sensitive device actuatable from an exterior surface of the token.

6. The apparatus of claim 5, wherein the input device comprises at least one push-button switch.

7. The apparatus of claim 1, further comprising:

an output device, communicatively coupled to the processor by a second path distinct from the USB-compliant interface, for prompting a user to provide an authorization of a processor operation.

8. The apparatus of claim 7, wherein the path and the second path are a common path.

9. The apparatus of claim 7, wherein the output device prompts the user to provide an authorization of the processor operation when processor operation requires access to the private data stored in the memory.

10. The apparatus of claim 7, wherein the output device comprises at least one light-emitting device.

11. The apparatus of claim 7, wherein the output device comprises at least one aural reproduction device.

12. The apparatus of claim 7, wherein the output device comprises at least one liquid crystal display (LCD).

13. The apparatus of claim 7, wherein the output device provides an alphanumeric message indicating that user input is required.

14. The apparatus of claim 13, wherein the alphanumeric message identifies the processing operation.

15. The apparatus of claim 13, wherein the alphanumeric message identifies a private key.

16. The apparatus of claim 1, wherein the memory is configured to store the data in at least one file, wherein:

the file belongs to a file type set comprising:

a data file type for storing non-private data;

a key file type for storing the private data;

the access to the file in the memory is classifiable according to an access type set including:

a read access type permitting data to be read from the file;

a write access type permitting data to be written to the file; and

the processor provides the conditional access to the memory according to the file type and the access type.

17. The apparatus of claim 16, wherein the processor provides conditional access to the memory according to:

	File Type		
Access Type	Data	Key	Counter
Read	Conditional Access	No Access	Conditional Access
Write	Conditional Access	Conditional Access	Conditional Access

18. A method of authorizing access to private data stored in a token having a processor communicatively coupleable to a host processor via a Universal Serial Bus (USB) interface, comprising the steps of:

accepting a command in the token invoking a processor operation;

accepting a user input signaling authorization of the processor operation via an input device; and

providing the user input to the processor via a communication path distinct from the USB-compliant interface.

19. The method of claim 18, further comprising the step of:

determining if the processor operation requires access to the private data stored in the token; and

prompting the user to authorize the processor operation via an output device communicatively coupled to the processor if the processor operation requires access to private data stored in a memory in the token;

20. The method of claim 19, wherein the output device is communicatively coupled to the processor by a second communication path distinct from the USB-compliant interface.

21. The method of claim 20, wherein the first path and the second path are common.

22. The method of claim 20, wherein the step of determining if the processor requires access to a private key stored in the token comprises the steps of:

determining which data stored in the memory is affected by the processor operation; and

determining whether the data affected by the processor operation is associated with an identification designating the data as a private key.

23. The method of claim 20, wherein the path is entirely internal to the token.

24. The method of claim 20, wherein the input device is a pressure-sensitive device actuatable from an exterior surface of the token.

25. The method of claim 24, wherein the input device is a push-button switch actuatable from an exterior surface of the token.

26. The method of claim 20, wherein the output device comprises at least one light emitting device.

27. The method of claim 20, wherein the output device comprises at least one aural reproduction device.

28. The method of claim 20 wherein the output device comprises at least one liquid crystal display.

29. The method of claim 20, wherein the step of prompting the user to authorize the processor operation via an output device comprises the step of:

providing an alphanumeric message indicating that user input is required.

30. The method of claim 29, wherein the alphanumeric message identifies the processing operation.

31. The method of claim 29, wherein the alphanumeric message identifies the private data.

32. The method of claim 20, wherein the memory is configured to store the data in at least one file, wherein:

the file belongs to a file type set comprising:

a data file type for storing non-private data;

a key file type for storing the private data;

the access to the file in the memory is classifiable according to an access type set including:

a read access type permitting data to be read from the file

a write access type permitting data to be written to the file

the processor provides the conditional access to the memory according to the file type and the access type.

33. The method of claim 32, wherein the processor provides conditional access to the memory according to:

	File Type		
Access Type	Data	Key	Counter
Read	Conditional Access	No Access	Conditional Access
Write	Conditional Access	Conditional Access	Conditional Access

34. The method of claim 20, wherein the command is an authorization request including a challenge value and the processor operation is a hash function using the challenge value and the private data.

35. A program storage device, readable by a computer, tangibly embodying at least one program of instructions executable by the computer to perform method steps of authorizing access to private data stored in a token having a processor communicatively coupleable to a host processor via a Universal Serial Bus (USB) interface, the method steps comprising the steps of:

accepting a command in the token invoking a processor operation;

determining if the processor operation requires access to the private data stored in the token;

prompting the user to authorize the processor operation via an output device communicatively coupled to the processor by a path distinct from the USB-compliant interface if the processor operation requires access to a private data stored in a memory in the token;

accepting a user input signaling authorization of the processor operation via an input device; and

providing the user input to the processor via a communication path distinct from the USB-compliant interface.

36. The program storage device of claim 35, wherein the first path and the second path are common.

37. The program storage device of claim 35, wherein the method step of determining if the processor requires access to a private key stored in the token comprises the steps of:

determining which data stored in the memory is affected by the processor operation; and

determining whether the data affected by the processor operation is associated with an identification designating the data as the private key.

38. The program storage device of claim 35, wherein the path is entirely internal to the token.

39. The program storage device of claim 35, wherein the input device is a pressure-sensitive device actuatable from exterior surface of the token.

40. The program storage device of claim 39, wherein the input device is a push-button switch actuatable from an exterior surface of the token.

41. The program storage device of claim 35, wherein the output device comprises at least one light emitting device.

42. The program storage device of claim 35, wherein the output device comprises at least one aural reproduction device.

43. The program storage device of claim 35, wherein the output device comprises at least one liquid crystal display.

44. The program storage device of claim 35, wherein the method step of prompting the user to authorize the processor operation via an output device comprises the method step of:

providing an alphanumeric message indicating that user input is required.

45. The program storage device of claim 44, wherein the alphanumeric message identifies the processing operation.

46. The program storage device of claim 44, wherein the alphanumeric message identifies the private data.

47. The program storage device of claim 40, wherein the memory is configured to store the data in at least one file, wherein:

the file belongs to a file type set comprising:

a data file type for storing non-private data;

a key file type for storing the private data;

the access to the file in the memory is classifiable according to an access type set including:

a read access type permitting data to be read from the file

a write access type permitting data to be written to the file

the processor provides the conditional access to the memory according to the file type and the access type.

48. The program storage device of claim 47, wherein the processor provides conditional access to the memory according to:

	File Type		
Access Type	Data	Key	Counter
Read	Conditional Access	No Access	Conditional Access
Write	Conditional Access	Conditional Access	Conditional Access

49. A compact personal token, comprising:

a USB-compliant interface releaseably coupleable to a host processing device;

a memory;

a processor, coupled to the memory and communicatively coupleable to the host processing device via the USB-compliant interface, the processor for providing the host processing device conditional access to store and retrieve data storable in the memory, the data including a personal identification private to the user; and

a user input device, communicatively coupled to the processor by a path distinct from the USB-compliant interface, for accepting a user input describing the personal identification.

50. The apparatus of claim 49, wherein the user input device comprises a character input device.

51. The apparatus of claim 50, wherein the character input device comprises a wheel having an input position for each character in an input character set.

52. The apparatus of claim 51, wherein each character is selected by depression of the wheel.

53. The apparatus of claim 48, wherein the user input device comprises a first pressure sensitive device actuatable from an exterior side of the token, and a second pressure sensitive device actuatable from the exterior side of the token, wherein actuation of the first pressure sensitive device selects a character from a character set, and actuation of the second pressure sensitive device enters the character as at least a portion of the personal identification.

54. A method of authentication using a token having a processor communicatively coupleable to a host processor via a Universal Serial Bus (USB) compliant interface, comprising the steps of:

accepting a user input comprising a personal identification via an input device; and

providing the user input to the processor via a communication path distinct from the USB-compliant interface.

55. The method of claim 54, further comprising the steps of:

accepting a command in the token invoking a processor operation;

determining if the processor operation requires access to the personal identification storable in a memory of the token; and

determining if the personal identification is stored in the memory of the token

prompting the user to enter a personal identification if the processor operation requires access to the personal identification and the personal identification is not stored in the memory of the token.

56. The method of claim 54, wherein the step of prompting the user to enter the personal identification number comprises the step of activating a user output device via second communication path distinct from the USB-compliant interface.

57. The method of claim 54, wherein the input device comprises a character input device.

58. The method of claim 57, wherein the character input device comprises a wheel having an input position for each character in an input character set.

59. The method of claim 58, wherein each character is selected by depression of the wheel.

60. The method of claim 54, wherein the user input device comprises a first pressure sensitive device actuatable from an exterior side of the token, and a second pressure sensitive device actuatable from an exterior side of the token, wherein actuation of the first pressure sensitive device selects a character from a character set, and actuation of the second pressure sensitive device enters the character as at least a portion of the personal identification.

61. A compact personal token, comprising:

a USB-compliant interface releaseably coupleable to a host processing device;

a memory;

a processor, communicatively coupled to the memory and communicatively coupleable to the host processing device via the USB-compliant interface, the processor for providing the host processing device conditional access to data storable in the memory; and

a user input device, communicatively coupled to the processor by a path distinct from the USB-compliant interface.

62. The apparatus of claim 61, wherein the user input device is configured to control an operation of the processor.

63. The apparatus of claim 61, wherein the operation comprises an operation selected from the group comprising:

an encryption operation; and

a decryption operation.

64. The apparatus of claim 61, wherein the operation comprises a digital signature operation using a private key stored in the memory.

65. The apparatus of claim 61, wherein the input device comprises at least one pressure-sensitive device actuatable from an exterior surface of the token.

66. The apparatus of claim 61, wherein the input device comprises at least one push-button switch.

67. The apparatus of claim 61, further comprising an output device, communicatively coupled to the processor by path distinct from the USB-compliant interface, for providing information regarding the operation of the processor.

68. The apparatus of claim 67, wherein the output device comprises at least one light emitting device.

69. The apparatus of claim 67, wherein the output device comprises at least one liquid crystal display.

70. The apparatus of claim 67, wherein the output device comprises at least one aural output device.

71. A method of authorizing access to private data stored in a token having a processor communicatively coupleable to a host processor via a Universal Serial Bus (USB) interface, comprising the steps of:

accepting a command in the token invoking a processor operation;

accepting a user input to control the processor operation via an input device; and

providing the user input to the processor via a communication path distinct from the USB-compliant interface.

72. The method of claim 71, wherein the operation comprises an operation selected from the group comprising:

an encryption operation;

a decryption operation; and

a digital signature operation using a private key.

73. The method of claim 71, wherein the user input device comprises at least one pressure sensitive device actuatable from an exterior surface of the token.

74. The method of claim 71, further comprising the step of:

prompting the user to control the processor operation via an output device communicatively coupled to the processor by a second path distinct from the USB-compliant interface.

75. The method of claim 74, wherein the path and the second path are common.

76. The method of claim 74, wherein the output device is selected from the group comprising:

a light emitting device;

an liquid crystal display; and

an aural reproduction device.

77. A compact personal token, comprising:

a USB-compliant interface releaseably coupleable to a host processing device;

a memory;

a processor, communicatively coupled to the memory and communicatively coupleable to the host processing device via the USB-compliant interface, the processor for providing the host processing device conditional access to data storable in the memory; and

a user output device, communicatively coupled to the USB-compliant interface.

78. The apparatus of claim 77, wherein the user output device is coupled to a power signal of the USB-compliant interface.

79. The apparatus of claim 77, wherein the user output device is coupled to a data signal of the USB-compliant interface.

80. A compact personal token, comprising:

a USB-compliant interface releaseably coupleable to a host processing device;

a memory;

a processor, communicatively coupled to the memory and communicatively coupleable to the host processing device via the USB-compliant interface, the processor for providing the host processing device conditional access to data storable in the memory; and

a user output device, communicatively coupled to the processor.

81. The apparatus of claim 80, wherein the user output device is coupled to the processor by a path distinct from the USB-compliant interface.

82. The apparatus of claim 80, wherein the user output device is configured to indicate the operation of the processor.

83. The apparatus of claim 80, wherein the operation comprises an operation selected from the group comprising:

an encryption operation;

a decryption operation; and

a digital signature operation using a private key.

84. The apparatus of claim 80, wherein the user output device is selected from a group comprising

at least one light emitting device;

at least one liquid crystal display.

at least one aural device.

85. The apparatus of claim 80, further comprising an input device, communicatively coupled to the processor by path distinct from the USB-compliant interface, for providing information for the operation of the processor.

86. A method of authorizing access to private data stored in a token having a processor communicatively coupleable to a host processor via a Universal Serial Bus (USB) interface, comprising the steps of:

accepting a command in the token invoking a processor operation; and

signaling the processor operation via a user output device.

87. The method of claim 86, wherein the operation comprises an operation selected from the group comprising:

an encryption operation;

a decryption operation; and

a digital signature operation using a private key.

88. The method of claim 86, wherein the user output device is communicatively coupled to the processor via a communication path distinct from the USB-compliant interface.

89. The method of claim 86, wherein the user output device is selected from the group comprising:

at least one light emitting device;

at least one liquid crystal display; and

an aural device.